Galois theory and algorithms for linear differential equations

Put, Marius van der

Published in:
Journal of symbolic computation

DOI:
10.1016/j.jsc.2004.11.013

Publication date:
2005

Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 39 (2005) 451–463
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Galois theory and algorithms for linear differential equations

Marius van der Put

Rijksuniversiteit Groningen, P.O. Box 800, 9700 AV Groningen, Netherlands

Received 2 September 2003; accepted 1 November 2004

Abstract

This paper is an informal introduction to differential Galois theory. It surveys recent work on differential Galois groups, related algorithms and some applications.

Keywords: Linear differential equations; Differential Galois groups; Direct and inverse problems; Descent for differential equations

1. An informal introduction

Differentiation of functions, integration and differential equations is a subject with a long history. It was, and still is, mainly a part of analysis. In the 20th century, algebraic approaches to the subject were developed by Picard, Painlevé, Vessiot, Ritt, Kolchin, Risch, Kaplansky, Katz, Deligne and many others. Liouville's work can be seen as an early successful attempt at applying algebraic methods to differential equations. He introduced elementary functions and gave a criterion for any second order, linear differential equation to have an elementary solution.

A first step, in modern terminology, is the notion of *differential field*. This is a field K, provided with a map $f \in K \mapsto f' \in K$, called a *differentiation* or a *derivation*, which has the properties $(f+g)' = f' + g'$ and $(fg)' = f'g + fg'$. In what follows we will suppose that K has characteristic zero and that its field of constants $C := \{a \in K \mid a' = 0\}$ is algebraically closed and distinct from K. Typical examples are:

E-mail address: mvdput@math.rug.nl.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2004.11.013

(i) Let C be any algebraically closed field of characteristic 0. Then $C(z)$, provided with the differentiation $f \mapsto \frac{\mathrm{d}f}{\mathrm{d}z}$, has the required properties.
(ii) C as above and $C((z))$ is the field of the formal Laurent series over C with differentiation given by $(\sum a_n z^n)' = \sum n a_n z^{n-1}$.
(iii) $\mathbf{C}$ denotes the field of the complex numbers and $\mathbf{C}(\{z\})$ denotes the field of the convergent Laurent series, provided with the differentiation given by the formula in (ii).
(iv) Let U be an open connected subset of $\mathbf{C}$. The field of the meromorphic functions on U, provided with the differentiation $f \mapsto \frac{\mathrm{d}f}{\mathrm{d}z}$, is a differential field with field of constants $\mathbf{C}$.

Also differential rings (the definition is obvious) have been studied. For general differential rings, differential Galois theory has not been developed, due to a lack of good algebraic properties of these rings. This holds especially for the ring of (say) the complex valued C^∞-functions on a connected real C^∞-manifold. Recently, Malgrange has developed Galois theory for non-linear differential equations in a setting which is a mixture of complex analytic and algebraic methods. In this survey, we will restrict ourselves to differential fields and linear differential equations.

Homogeneous linear differential equations over a differential field K can be represented in various ways, for example:

(1) *Scalar or operator form.* A differential operator over K has the form $a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_1\partial + a_0$ with $a_n, \ldots, a_0 \in K$. Here ∂ stands for the operator $f \mapsto f'$ on the field K. The skew ring of the differential operators over K is denoted by $K[\partial]$. A (homogeneous) scalar differential equation has the form $L(y) = 0$ with $L \in K[\partial]$.
(2) *Matrix form.* For a vector $Y \in K^n$, one writes Y' for the vector obtained by differentiating all the entries of Y. One associates with any matrix $A \in \mathrm{Matr}(n, K)$ the matrix differential equation $Y' + AY = 0$.
(3) *Module form.* A differential module $M = (M, \partial)$ over K is a finite dimensional K-vector space M provided with a C-linear map $\partial : M \to M$ satisfying $\partial(fm) = f'm + f\partial m$. The "equation" reads $\partial m = 0$.

The relations between these notions are as follows. Let a scalar equation $L(y) = 0$ with $L \in K[\partial]$ of degree $n \geq 1$ be given. One defines the vector $Y = (y, y', \ldots, y^{(n-1)})^t$ and translates the given equation into $Y' + AY = 0$, with an obvious matrix A (the companion matrix of L is $-A$). For a given matrix equation $Y' + AY = 0$, one defines the differential module $M = (M, \partial)$ by $M = K^n$ and ∂ is the operator $Y \mapsto Y' + AY$. Finally, any differential module (M, ∂) can be seen as a left module over $K[\partial]$ from the formula $(\sum a_i\partial^i)m = \sum_i a_i\partial^i(m)$. This left module has finite dimension, say n, over K. Properties of the skew ring $K[\partial]$ imply that M is generated as a left module by a single element e (called a cyclic vector). One associates with M and e the monic $L \in K[\partial]$ of degree n with $Le = 0$.

The solution space of an equation is given by:

Scalar form, $y \in K$ with $L(y) = 0$ (with degree of L is n).
Matrix form, $Y \in K^n$ with $Y' + AY = 0$.
Module form, $m \in M$ with $\partial m = 0$ (with $\dim_K M = n$).

In each case, the solution space is a vector space over C of dimension $\leq n$. If this dimension is equal to n, then we lose interest in the equation and the equation is called *trivial*. If the dimension of the solution space is strictly less than n, then one would like to find a larger differential ring (or differential field) where the solution space has dimension n. This situation is rather analogous to the formation of the splitting field of a polynomial equation. The "smallest" differential ring extension R of K such that the equation has a solution space of dimension n over C is called a *Picard–Vessiot ring* (for short, PVR) for the equation over K. This ring exists, is unique (up to isomorphism) and is an integral domain. Its field of fractions is called the *Picard–Vessiot field* (for short, PVF) of the equation over K. The definition of a Picard–Vessiot ring R for, say, a matrix differential equation $Y' + AY = 0$ over K is as follows:

(i) R is a K-algebra with a differentiation, extending that of K.
(ii) Let $I \subset R,\ I \neq R$ be an ideal, invariant under the differentiation of R; then $I = \{0\}$.
(iii) There is a matrix $F \in \mathrm{GL}(n, R)$ (called a fundamental matrix), satisfying $F' + AF = 0$.
(iv) R is generated over K by the entries of F and the inverse of $\det(F)$.

We note that the columns of F form a basis over C of the solution space of the matrix equation over R, the PVR. For a differential module M over K, the PVR is defined in a similar way. Properties (i) and (ii) remain the same. Property (iii) now reads: $V := \ker(\partial, R \otimes_K M)$ has dimension n over C. Property (iv) is replaced by the following. A C-basis of V is expressed in a basis of M over K. Let H be the resulting matrix. Then R is generated over K by the entries of H and the inverse of $\det(H)$.

The *differential Galois group* of a differential module M over K is the group $G = \mathrm{Gal}(\mathrm{PVR}/K)$ of all K-linear automorphisms of PVR commuting with the differentiation of PVR. Some important results are:

G acts faithfully on the solution space $V := \ker(\partial, \mathrm{PVR} \otimes_k M)$. The embedding $G \subset \mathrm{GL}(V)$ makes G into a linear algebraic group. Moreover, there exists a finite Galois extension $L \supset K$ such that $L \otimes_K \mathrm{PVR}$ is isomorphic to $L \otimes_C C[G]$ (here $C[G]$ denotes the coordinate ring of G).

Examples. C is an algebraically closed field of characteristic 0 and the differential field is $K = C(z)$ with derivation $\frac{\mathrm{d}}{\mathrm{d}z}$.

(1) $y' = \frac{a}{z} y$ with $a \in C^*$.
  (a) If $a \notin \mathbf{Q}$, then $\mathrm{PVR} = K[T, T^{-1}]$ with $T' = \frac{a}{z} T$. The differential Galois group is isomorphic to the multiplicative group C^* and consists of the maps $\sigma : \mathrm{PVR} \to \mathrm{PVR}$ with $\sigma T = cT$.
  (b) If $a = \frac{i}{n}$, $(i, n) = 1$, then $\mathrm{PVR} = K[t] = K[T]/(T^n - z^i)$. The differential Galois group is isomorphic to μ_n and consists of the σ with $\sigma t = ct$ and $c^n = 1$.
(2) $M = Ke_1 \oplus Ke_2$, $\partial e_1 = 0,\ \partial e_2 = f e_1$ with $f \in K$.
  This corresponds to the inhomogeneous equation $y' = f$. If there is no solution in K, then $\mathrm{PVR} = K[T]$ and $T' = f$. The differential Galois group is isomorphic to the additive group C and consists of the automorphisms σ with $\sigma T = T + c$.
(3) $y'' = zy$, this is the Airy equation.

It is not so easy to prove that PVR $= K[y_1, y_2, y_1', y_2']$ with only one relation, namely $y_1y_2' - y_1'y_2 = 1$. The solution space is $Cy_1 + Cy_2$; the differential Galois group is isomorphic to $\mathrm{SL}(2, C)$. The action of this group on PVR is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} y_1 = ay_1 + by_2 \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} y_2 = cy_1 + \mathrm{d}y_2,$$

and the same formulas for the action on y_1', y_2'.

2. More on differential Galois groups

2.1. Interpretation of the Picard–Vessiot ring and the differential Galois group

An explicit description of the PVR and the differential Galois provides, in principle, all algebraic information on the solutions. For instance, in example (3) of Section 1, one interprets y_1, y_2 as the two Airy functions, which are entire functions on $\mathbf{C}$ and solutions of $y'' = zy$. It follows that the only algebraic relation between the functions z, y_1, y_2, y_1', y_2' is $y_1y_2' - y_1'y_2 = 1$.

2.2. Finite differential Galois groups

The differential Galois group of an equation is *finite* if and only if all its solutions are algebraic over the differential field K. Algebraic solutions of a differential equations are of course rather interesting. An inspiration for much research (B. Dwork, N. Katz, D. Chudnowski, G. Chudnovsky, Y. André et al.) on algebraic solutions is *Grothendieck's conjecture*. In simplified form this reads as follows:
Let $L(y) = 0$ be a differential equation over $\mathbf{Q}(z)$ of order n. Then all its solutions are algebraic if for all prime numbers p, with the exception of finitely many, the reduction modulo p of this equation has n independent solutions in $\mathbf{F}_p(z)$.

2.3. Formal differential equations

A differential module (or linear differential equation) over the differential field $\mathbf{C}((z))$ is called a formal differential equation. It is may appear surprising that one can actually classify these modules. A possible formulation, involving roots of the variable z and in terms of matrix differential equations is as follows. Take integers $n, e \geq 1$ and a polynomial q in the variable $z^{-1/e}$ (e.g., $2 + z^{-1/3} + z^{-7/6}$). With these data one associates the matrix differential equation of size n

$$z\frac{\mathrm{d}}{\mathrm{d}z} + \begin{pmatrix} q & 1 & 0 & \cdot & \cdot & \cdot \\ 0 & q & 1 & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & 0 & q & 1 \\ \cdot & \cdot & \cdot & \cdot & 0 & q \end{pmatrix}.$$

This is actually a matrix differential equation over the field $\mathbf{C}((z^{1/e}))$. Moreover, this matrix differential equation is indecomposable, in the sense that it is not equivalent to the direct

sum of two other matrix differential equations. The classification theorem states that every matrix differential equation over $\mathbf{C}((z))$ is, considered as an equation over $\mathbf{C}((z^{1/e}))$ (for a suitable $e \geq 1$), equivalent to a direct sum of the indecomposable matrix differential, defined above. This result looks somewhat like the Jordan normal form for matrices. The differential Galois group can easily be read off from this standard form. Indeed, solving the matrix differential equation in standard form is equivalent to solving some order 1 equations $z\frac{\mathrm{d}}{\mathrm{d}z}y = q_i y$ for $i = 1, \ldots, r$ with $q_1, \ldots, q_r$ polynomials in $z^{-1/e}$ and possibly the equation $z\frac{\mathrm{d}}{\mathrm{d}z}y = 1$ (if there are non-trivial "Jordan blocks"). There are efficient algorithms that compute this standard form. M. van Hoeij has implemented (in MAPLE) a factorization algorithm for differential operators over $\mathbf{C}((z))$. Using a cyclic vector, this algorithm yields the standard form of a matrix differential equation over $\mathbf{C}((z))$. M. Barkatou and E. Pflügel have implemented (in ISOLDE) an algorithm in terms of matrix differential equations over $\mathbf{C}((z))$.

2.4. Meromorphic differential equations

A meromorphic differential equation is, say, a matrix differential equation $z\frac{\mathrm{d}Y}{\mathrm{d}z} + AY = 0$ over the field of convergent Laurent series $\mathbf{C}(\{z\})$. There is a transformation $T \in \mathrm{GL}(n, \mathbf{C}((z)))$ which brings it into the standard form $z\frac{\mathrm{d}Z}{\mathrm{d}z} + BZ = 0$, considered above. Explicitly: write $Y = TZ$ with Z a vector; then the equation becomes $z\frac{\mathrm{d}Z}{\mathrm{d}z} + (zT^{-1}T' + AT)Z = 0$. This equation is supposed to be the standard form $z\frac{\mathrm{d}Z}{\mathrm{d}z} + BZ = 0$.

We emphasize that T is in general *divergent*. At this point the classical analysis of divergent power series comes into the picture. The classical notion of Borel summation has been transformed by J. Écalle, J. Martinet, J.-P. Ramis, B.L.J. Braaksma and many others, into a powerful tool, called *multisummation*. For a "non-singular" direction d at the origin $z = 0$, one forms the multisum $\mathrm{sum}_d(T)$ in the direction d. The result is a matrix, whose coefficients are meromorphic functions on a certain sector around d. The asymptotic behaviour of $\mathrm{sum}_d(T)$ in this sector is T and, moreover, the matrix $\mathrm{sum}_d(T)$ transforms $z\frac{\mathrm{d}Y}{\mathrm{d}z} + AY = 0$ into $z\frac{\mathrm{d}Z}{\mathrm{d}z} + BZ = 0$, too. There are finitely many singular directions. If one jumps over a singular direction, then the multisum of T changes. It changes in fact by multiplication with a constant matrix St_d, called the *Stokes matrix for the singular direction* d. The standard form $z\frac{\mathrm{d}Z}{\mathrm{d}z} + BZ = 0$ prescribes the possible singular directions and the form of St_d (i.e., $St_d - 1$ is a rather special nilpotent matrix). As Stokes writes in a letter of March 19, 1857, to the woman who was to become Lady Stokes, he found this phenomenon at 3 o'clock in the morning while studying the asymptotic properties of the solutions of the Airy equation near the singular point $z = \infty$. This famous letter starts with:

When the cat's away the mice may play. You are the cat and I am the poor little mouse. I have been doing what I guess you won't let me do when we are married, sitting up till 3 o'clock in the morning fighting hard against a mathematical difficulty.

The Stokes matrices play a central role for meromorphic differential equations. We illustrate this with two theorems, due to J. Martinet and J.-P. Ramis. They are:

The differential Galois group of a matrix differential equation over $\mathbf{C}(\{z\})$ *is the smallest algebraic group that contains the differential Galois group of this equation over the field* $\mathbf{C}((z))$ *(this group is easily computable) and the Stokes matrices for all singular directions.*

The equivalence class of a matrix differential equation $z\frac{dY}{dz} + AY$ *is completely determined by its formal equivalence class and the Stokes matrices* $\{St_d\}$. *Moreover, any formal equivalence class and any collection of "admissible" unipotent matrices* $\{S_d\}$ *comes from a meromorphic matrix differential equation.*

Stokes actually computed for the Airy equation, at the singular point $z = \infty$, the Stokes matrices. Precious few explicit examples of Stokes matrices are known. In the "generic situation" the Stokes matrix St_d is known to have 1's on the diagonal and possibly one non-zero entry, say y, at a prescribed place (i, j) with $i \neq j$. Most of the time one only wants to know whether y is zero or not. The calculation of y involves a sequence of Laplace and Borel transforms and analytic continuation of some analytic functions along half-lines starting at $z = 0$. No algorithm (efficient or not) for this computation seems available. It is an interesting open problem whether at least a theoretical algorithm for the computation of Stokes matrices is possible.

2.5. Monodromy and the differential Galois group

Let a matrix differential equation $\frac{dY}{dz} + AY = 0$ of size n over the field $\mathbf{C}(z)$ be given. This is a linear differential equation on the projective line over $\mathbf{C}$. Let $a_1, \ldots, a_s$ denote the singular points of the equation. For convenience we suppose that $0 \notin \{a_1, \ldots, a_s\}$. Let π_1 denote the fundamental group of $X := \mathbf{P}^1_{\mathbf{C}} \setminus \{a_1, \ldots, a_s\}$ with base point 0. The solution space, locally at $z = 0$, is a vector space V of dimension n over $\mathbf{C}$. Analytic continuation of the solutions in V, along any path λ in X, starting at $z = 0$, yields solutions of the equation locally at the end point of λ. In this way, one obtains a homomorphism $\rho : \pi_1 \to \mathrm{GL}(V)$, which is called the monodromy map. The image of ρ in $\mathrm{GL}(V)$ is called the monodromy group. It turns out that the monodromy group is a subgroup of the differential Galois group. Moreover, if all the singularities are regular singular, then the Zariski closure of the monodromy group is equal to the differential Galois group.

Numerical computations of the monodromy are possible, but yield rather uncertain results. In some cases, e.g., when one knows that the monodromy matrices have integral coefficients w.r.t. a special basis, an exact computation of the monodromy group is possible. However, in many cases, an exact computation of the differential Galois group is possible. This is the observation that led to an application (by J.J. Morales-Ruiz, J.-P. Ramis and others) of differential Galois theory to the problem of deciding whether certain Hamilton systems are completely integrable.

3. The direct problem

The calculation of the Picard–Vessiot ring and the differential Galois group of a given linear differential equation or a given differential module is called the *direct problem*. Many practical and efficient algorithms have been developed. The basic idea, already present in Beke's classical work, can best be explained with the *Tannaka approach* to differential equations. For differential modules there are constructions of linear algebra, e.g., tensor product, duals, submodules, quotients. Applied to a fixed differential module M, this yields a category $\{\{M\}\}$ of differential modules whose objects are obtained from M by the above constructions of linear algebra. For integers $a, b \geq 0$ one defines the differential M_b^a as the

tensor product of a copies of the dual M^* of M and of b copies of M itself. Let $N_1 \subset N_2$ be submodules of a finite direct sum $\oplus_i M_{b_i}^{a_i}$; then N_2/N_1 is an object of $\{\{M\}\}$. Moreover, every object of this category is obtained in this way. There is a strong connection between $\{\{M\}\}$ and the differential Galois group G of M. Let Repr_G denote the category of the representations of G on finite dimensional vector spaces over C. This is expressed in the following *Tannaka correspondence*:

There is an equivalence $S : \{\{M\}\} \to \mathrm{Repr}_G$ *of categories which respects all constructions of linear algebra.*

The *definition of* S is as follows. Let PVR be the Picard–Vessiot ring of M. For any object N of $\{\{M\}\}$ of dimension d over K, the solution space $S(N) =: \ker(\partial, \mathrm{PVR} \otimes_K N)$ has dimension d over C. The action of G on PVR induces an action on $\mathrm{PVR} \otimes_K N$ which commutes with differentiation and thus with ∂. Hence G acts on the C-vector space $S(N)$. This makes $S(N)$ into a representation of G. In particular, the differential module M itself is mapped by S to the solution space $V := \ker(\partial, \mathrm{PVR} \otimes_K M)$ with its G-action. Some differential Galois theory is needed to show that S is an equivalence of categories commuting with all constructions of linear algebra.

3.1. Is the differential Galois group computable?

Now we specialize to a differential field of the form $K = C(z)$, with C an algebraically closed field, that is suitable for computations (e.g., the algebraic closure of **Q**). Let N be a differential module over K. There are effective algorithms for the computation of:

(a) $\ker(\partial, N)$ (rational solutions).
(b) The one-dimensional submodules of N (rational solutions of the Riccati equation).
(c) The d-dimensional submodules of N (this amounts to calculating the one-dimensional "decomposable" submodules of the exterior power $\Lambda^d N$ of N).

We try to combine this with the above Tannaka correspondence in order to compute, say, the differential Galois group of a given differential module M. Note that the Picard–Vessiot ring PVR and the solution space V are both unknown! The submodules of M are in 1–1 correspondence with the G-invariant subspaces of V. The same statement holds for any finite direct sum $\oplus_i M_{b_i}^{a_i}$ and the C-vector space $\oplus_i V_{b_i}^{a_i}$. Write $M(d)$, with $d \geq 1$, for the direct sum $\oplus_{a \leq d,\ b \leq d} M_b^a$. A complete list of the submodules of all $M(d)$ determines the differential Galois group (and the Picard–Vessiot ring, too). The knowledge of the submodules of $M(d)$ provides an algebraic subgroup $G(d)$ of $\mathrm{GL}(V)$, such that $G \subset G(d)$. By construction, $G(d+1) \subset G(d)$. What is missing for making this into a "theoretical" algorithm is a criterion that can be used to decide whether, for a given d, the group G is equal to $G(d)$. Recently, the existence of such a criterion has been shown by Hrushovski (2002). Some delicate properties of linear algebraic groups go into his proof. Because of his use of an involved logical language developed for differential equations, the proof is not fully understood.

3.2. Explicit algorithms

The first efficient algorithm for order two equations over $K = C(z)$ is due to J. Kovacic. Let a differential module M of dimension 2 over K be given. For convenience, we suppose

that the differential Galois group G is contained in $\mathrm{SL}(V) = \mathrm{SL}(2, C)$. The (conjugacy classes of the) algebraic subgroups of $\mathrm{SL}(V)$ have a simple classification. In particular, the various algebraic subgroups of $\mathrm{SL}(V)$ are essentially distinguished by the existence of invariant lines for their actions on the symmetric powers $\mathrm{sym}^i V$ for $i = 1, 2, 4, 6, 12$. Thus a computation of the one-dimensional submodules of $\mathrm{sym}^i M$ for $i = 1, 2, 4, 6, 12$ suffices for the determination of the differential Galois group and the Picard–Vessiot ring.

This method has been extended to equations of order 3 (and higher) in a more or less systematic way. M. van Hoeij has announced (June 2003) an implementation in MAPLE for order 3 (imprimitive) differential equations. A full implementation for order 3 equations was announced (September 2003) by M. Bronstein (http://www-sop.inria.fr/cafe/Manuel.Bronstein/sumit/bernina).

Usually, for computations, C is a number field. A priori, the computation takes place in an algebraic closure $\overline{C}$ of C. One of the technical complications, already present for order 2 equations, is that one has to avoid large extensions of C. The latest ideas (Berkenbosch et al., 2003) for the implementation of the order 2 equations $y'' = ry$ with $r \in C(z)$ and the calculation of the differential Galois group G can be explained as follows:

(i) If there is a solution $u \in \overline{C}(z)$ of the Riccati equation $u' + u^2 = r$, then the differential Galois group is contained in an upper triangular group. In the above terminology, this means that $\mathrm{sym}^1 M$ has a proper submodule. This case is easy to handle and not very interesting (except for the "apparent singularities" of the solutions).

(ii) If there is a solution u in a quadratic extension of $\overline{C}(z)$ then the differential Galois group is contained in the infinite dihedral group $D_\infty^{\mathrm{SL}_2}$. In the above terminology, $\mathrm{sym}^2 M$ has a one-dimensional submodule. The computation of u poses no serious problems. For the determination of the differential Galois group (either $D_\infty^{\mathrm{SL}_2}$ or $D_n^{SL_2}$ with $n \geq 2$), one has to compute the order (either ∞ or n) of a certain divisor on the hyperelliptic curve with function field $\overline{C}(z)(u)$. The same problem occurs in the Risch algorithm for integration. It is solved by reducing this curve modulo two distinct primes.

(iii) In the remaining cases, G is equal to SL_2 or to one of the finite primitive subgroups $A_4^{SL_2}$, $S_4^{SL_2}$, $A_5^{SL_2}$ of SL_2. The first case is again not interesting, but can only be confirmed after excluding these finite groups.

The above finite primitive groups form the interesting case and the most complicated one for computation. One may suspect, from reducing the equation $y'' = ry$ modulo many small primes, that the differential Galois group is one of these finite primitive groups. An inspection of the "local exponents" is useful for guessing which finite primitive group G is the candidate. For each G (here one may include the imprimitive groups $D_n^{SL_2}$) there is a standard hypergeometric differential equation $\mathrm{St}_G = (\frac{\mathrm{d}}{\mathrm{d}t})^2 + a$ with $a \in \mathbf{Q}(t)$. Klein's theorem states that there exists a homomorphism of fields $\phi : \mathbf{Q}(t) \to \overline{C}(z)$ such that the pullback $\phi_* \mathrm{St}_G$ is, after normalization, equal to $(\frac{\mathrm{d}}{\mathrm{d}z})^2 - r$. The algorithm provides a direct computation of the pullback function ϕ. This function involves an extension of C of at most degree 3.

3.3. Complexity

We recall that $K[\partial]$ is the skew ring of the differential operators with coefficients in the differential field $K = C(z)$ and C is, say, the algebraic closure of $\mathbf{Q}$. Almost all calculations and implementations are formulated in terms of factoring differential operators. D.Yu. Grigoriev has made an analysis of the complexity of the factoring algorithm and finds an estimate which is "double exponential". Suppose that $L = L_1L_2$ is a factorization of a monic $L \in K[\partial]$ as a product of monic operators. The two factors L_1, L_2 may have many more singular points than L itself. These new "apparent singularities" contribute to the high estimate of the complexity because there could be exponentially many of them. An example of this phenomenon is given by the operator $L_d := \partial^2 - z^2 - (2d + 1)$ with d a positive integer. The unique monic right hand factor of L_d is $\partial - z - \frac{F_d'}{F_d}$, where F_d is the monic polynomial of degree d satisfying $F_d'' + 2zF_d' - 2dF_d = 0$.

We note, in passing, that factoring in terms of differential modules M over K (or connections on the projective line over C) could have a better complexity. Indeed, the set of the singular points of a differential submodule $N \subset M$ is contained in the set of singular points of M.

In contrast to the above, factoring in $\mathbf{Q}(z)[\partial]$ has an unknown complexity which seems to be at least as high as the complexity of the factorization in $\mathbf{Z}$. The following statement would, if true, prove this claim.

Let N be the product of two distinct prime numbers p, q. There exists a monic operator of degree 4, whose factorization in $\mathbf{Q}(z)[\partial]$ yields the factorization $N = pq$.

What can actually be shown is the following slightly weaker statement. For every positive integer a such that a is a square modulo N and N is a square modulo a, there is a monic operator $L \in \mathbf{Q}(z)[\partial]$ of degree 4 such that the decomposition of L as a product of two monic operators of degree 2 yields an integer b such that $b^2 \equiv a$ modulo N.

3.4. Descent theory

What lies behind this phenomenon is descent theory (see the preprint of van Hoeij and van der Put (2002)). The best way to formulate descent theory is by means of differential modules. However, it is more easily explained with differential operators. Let $C \supset \mathbf{Q}$ be a Galois extension. Two operators $L_1, L_2 \in C(z)[\partial]$ of the same degree n are called equivalent if $L_1A = BL_2$ for some non-zero $A, B \in C(z)[\partial]$ of degrees $<n$. The Galois group $G = \mathrm{Gal}(C/\mathbf{Q})$ acts on $C(z)[\partial]$. Suppose that a monic operator $L \in C(z)[\partial]$ has the property that $\sigma(L)$ is equivalent to L for all $\sigma \in G$. Does it follow that L is equivalent to a monic operator in $\mathbf{Q}(z)[\partial]$?

The answer is negative. The question leads to Galois cohomology and in particular to *skew differential fields* and differential equations over these fields. The basic *example* is:

The skew field of Hamilton's quaternions over $\mathbf{Q}$ is denoted by $\mathbf{H}$. Thus $\mathbf{H}$ has a basis $1, i, j, k$ over $\mathbf{Q}$ with, as usual, $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$. Then $F := \mathbf{Q}(z) \otimes_{\mathbf{Q}} \mathbf{H}$ is again a skew and this field is given a differentiation via the formula $(f \otimes h)' = f' \otimes h$ for any $h \in \mathbf{H}$ and $f \in \mathbf{Q}(z)$. The differentiation on F is $\mathbf{Q}$-linear and $(ab)' = a'b + ab'$ for all $a, b \in F$. Such a field will be called a skew differential field.

An order 1 differential equation over F has the form $y' + yd = 0$ for some $d \in F$. If one writes y as $y = y_0 \otimes 1 + y_1 \otimes i + y_2 \otimes j + y_3 \otimes k$ with $y_0, \ldots, y_3 \in \mathbf{Q}(z)$, then one finds a matrix differential equation for $(y_0, \ldots, y_3)^t$ and also a monic differential operator $L_4 \in \mathbf{Q}(z)[\partial]$ of degree 4. For the choice $d = (i + jz)$ one calculates

$$L_4 = \partial^4 + (2 + 2z^2)\partial^2 + 4z\partial + (4 + 2z^2 + z^4).$$

From the construction it follows that L_4 is irreducible over $\mathbf{Q}(z)$ and it is a product of two absolutely irreducible operators of order 2 in $\mathbf{Q}(\sqrt{-m})(z)[\partial]$ if and only if $m > 0$ is the sum of three squares in $\mathbf{Q}$. For $m = 1$ one obtains the right hand factor $L_2 \in \mathbf{Q}(i)(z)[\partial]$ of L_4

$$L_2 = \partial^2 - z^{-1}\partial + (iz^{-1} + 1 + z^2).$$

From the construction it follows that L_2 is equivalent to its complex conjugate and that L_2 is not equivalent to any operator in $\mathbf{Q}(z)[\partial]$. The object $\mathbf{H}$ is a quaternion algebra over $\mathbf{Q}$. A quaternion algebra $\mathbf{K}$ over $\mathbf{Q}$ is either a skew field or is isomorphic to the matrix algebra Matr$(2, \mathbf{Q})$. Let N be a product of two distinct primes p, q and let a be a positive integer with g.c.d.$(a, N) = 1$. Suppose that a is a square modulo N and that N is a square module a. One can construct a quaternion algebra K, isomorphic to Matr$(2, \mathbf{Q})$, such that the explicit isomorphism $K \to$ Matr$(2, \mathbf{Q})$ yields a non-zero rational solution (x, y, z) of $ax^2 + Ny^2 - z^2 = 0$. In particular, a square root of a modulo N is obtained. A suitable differential equation of order 1 over the differential quaternion ring $\mathbf{Q}(z) \otimes K$ yields, as above, a monic operator $L \in \mathbf{Q}(z)[\partial]$ of degree 4. The factorization of L as a product of two monic irreducible operators of degree 2 yields an explicit isomorphism $K \to$ Matr$(2, \mathbf{Q})$.

4. Inverse problems

4.1. Inverse problems over $C(z)$

As before, K is a differential field and its field of constants C is algebraically closed and has characteristic 0. Given a linear algebraic group G and a faithful representation W of G, one asks for a differential equation over K such that the action of its Galois group on the solution space is isomorphic to the G-module W. This is called the "inverse problem". C. Tretkoff and M. Tretkoff solved this problem for the case $K = \mathbf{C}(z)$, by constructing a finitely generated, Zariski dense subgroup H of G. The fundamental group π_1 of $\mathbf{P}^1_{\mathbf{C}} \setminus S$ for some finite set S admits a surjective homomorphism $\rho : \pi_1 \to H$. According to the classical Riemann–Hilbert correspondence, there is a regular singular differential equation over $\mathbf{C}(z)$, with H as monodromy group. The differential Galois group of this equation is the Zariski closure of H and therefore equal to G. This is however not the end of the story, since one is interested in a "constructive" solution of the problem.

A constructive solution for the case $K = C(z)$ and connected groups G was given by M.F. Singer and C. Mitschi. Recently J. Hartmann has presented a constructive solution for $K = C(z)$ and general G, under the assumption that for any finite group H a Galois extension of $C(z)$ with Galois group H is given.

Efficient algorithms for the inverse problem with $K = C(z)$ and finite groups G have been developed by F. Ulmer and M. van der Put. In particular, many order 3 differential operators with prescribed finite differential Galois group were computed.

4.2. Inverse problems for Riemann surfaces

One considers pairs (X, S) consisting of a compact Riemann surface X and a finite subset S of X. The question is which linear algebraic groups G can be realized as differential Galois group for a linear differential equation on X with singularities in the set S. Using analytic (and not constructive) methods, J.-P. Ramis were able to give the following answer:

Let $L(G)$ be the subgroup of G generated by its maximal tori. Then G can be realized for the pair (X, S) if and only if there is a morphism $\pi_1(X \setminus S) \to G/L(G)$ having a Zariski dense image.

4.3. The inverse problem for $K = \mathbf{C}(\{z\})$

We recall that $\mathbf{C}(\{z\})$ is the field of the convergent Laurent series over $\mathbf{C}$. J. Martinet and J.-P. Ramis solved the inverse problem for this field, using multisummation and Stokes matrices. The result is:

G is a differential Galois group for the field $\mathbf{C}(\{z\})$ if and only if $G/L(G)$ has a Zariski dense cyclic subgroup.

This result can in fact be derived from the inverse problem for Riemann surfaces by using the pair $(\mathbf{P}^1_{\mathbf{C}}, \{0, \infty\})$. Indeed, by a theorem of G.D. Birkhoff, any differential module over $\mathbf{C}(\{z\})$ is analytically equivalent to a differential equation on $\mathbf{P}^1_{\mathbf{C}}$, having any singularity at 0 and a regular singularity at ∞ (and no other singularities).

An even more complicated question concerns the description of the *universal differential Galois group*. In general, a differential field K has a universal Picard–Vessiot field $U \supset K$. This is the smallest differential field containing K, having C as field of constants and such that every linear differential equation over K has a fundamental matrix with coefficients in U. One can view U as the differential analogue of the algebraic closure of a field. The group G of the K-linear differential automorphisms of U is called the universal differential Galois group. G is an affine group scheme over C, or, stated differently, G is the projective limit of the linear algebraic groups that occur as differential Galois groups over K. For both fields $K = \mathbf{C}(\{z\})$ and $\widehat{K} = \mathbf{C}((z))$ (i.e., the field of all formal Laurent series) an explicit universal Picard–Vessiot field and explicit universal differential Galois groups, say G_{conv} and G_{formal}, can be described. For the affine group scheme G_{formal} this is not difficult. The connection between the two universal groups is given by an exact sequence of affine group schemes

$$1 \to N \to G_{\text{conv}} \to G_{\text{formal}} \to 1,$$

which admits a section. The main result is the description of the connculation fine group N, or rather of its Lie algebra. This reads as follows:

The Lie algebra of N is the completion of the universal free locally nilpotent Lie algebra on an infinite set of generators, namely the alien derivations introduced by J. Écalle.

This result rather resembles the Shafarevich conjecture concerning the Galois group G of $\overline{\mathbf{Q}}$ over its maximal cyclotomic subfield $\mathbf{Q}(\mu_\infty)$. The conjecture states:

G is the "nilpotent completion" of a free group on a countable number of (explicit) generators.

5. Comparison with other Galois theories

There are other classes of equations, having many features in common with linear differential equations. We only mention: Linear difference equations, Iterated differential equations in positive characteristic and Coverings of algebraic varieties in positive characteristic. For the first two categories, there exists an adequate Galois theory. The Galois groups are again linear algebraic groups over a field of constants. For the last category, ordinary Galois theory with finite or profinite groups plays a central role. Two interesting results are:

A recent theorem (Di Vicio, 2002) concerns q-difference equations over the field $\mathbf{Q}(z)$ (and with $q \in \mathbf{Q},\ q \neq 0, 1, -1$). It is a positive answer to Grothendieck's conjecture on p-curvatures in the setting of q-difference equations.

A linear q-difference equation

$$y(q^n z) + a_{n-1}(z)y(q^{n-1}z) + \cdots + a_0(z)y(z) = 0$$

has n independent solutions in $\mathbf{Q}(z)$ if (and only if) for almost all prime numbers p the reduction of this equation modulo p has n independent solutions in $\mathbf{F}_p(z)$.

We note that there is no good formulation of Grothendieck's conjecture for ordinary difference equations.

The second result answers a question posed by Abhyankar. The theorem is due to M. Raynaud and D. Harbater. Its formulation is strikingly similar to J.-P. Ramis' solution of the inverse problem for Riemann surfaces.

X is a smooth irreducible projective curve over an algebraically closed field of characteristic $p > 0$, $S \subset X$ a finite non-empty subset. Let G be a finite group and denote by $p(G)$ the subgroup generated by its p-Sylow subgroups. Then G is the Galois group of a cover $Y \to X$, ramified at most at S if and only if there is a surjective morphism $\pi_1^{(p)}(X \setminus S) \to G/p(G)$.

For more details on some of the topics discussed in this survey, and especially for bibliographic items, we refer the reader to the book (van der Put and Singer, 2003).

Acknowledgement

I would like to thank Mark van Hoeij for several improvements of this paper.

References

Di Vicio, L., 2002. Arithmetic theory of q-difference equations. Invent. Math. 150, 517–578.

Hrushovski, E., 2002. Computing the Galois group of a linear differential equation. In: Crespo, T., Hajto, Z. (Eds.), Differential Galois Theory, vol. 58. Banach Center Publ., pp. 97–138.

van der Put, M., Singer, M.F., 2003. Galois Theory of Linear Differential Equations. In: Grundlehren der mathematische Wissenschaften, vol. 328. Springer Verlag, Berlin.
Berkenbosch, M., van Hoeij, M., Weil, J.-A., 2003. Algorithms for order two differential equations (preprint).
van Hoeij, M., van der Put, M., 2002. Descent for differential modules and skew fields (preprint).